**Using MBSA Software list all the security updates missing in Window OS**

**What is MBSA (Microsoft Baseline Security Analyzer)?**

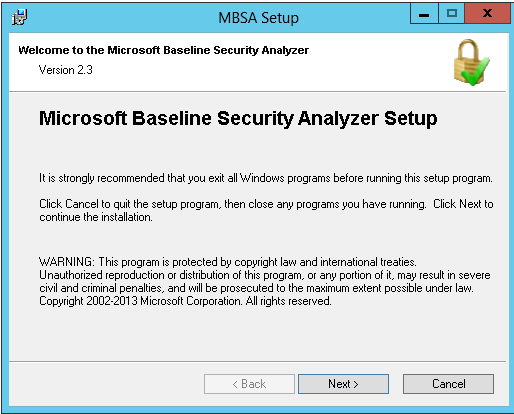
Microsoft Baseline Security Analyzer is one of the tools provided by Microsoft to help administrators to scan systems (local and remote) for missing security updates and common security misconfigurations. It can scan the server operating system and SQL Server but also other products as well, such as Microsoft web server IIS.

## Installation procedure –

Once the files have been downloaded, put them on the server you’ll use as a host for the tool, or on a network share and go to the server of your choice.

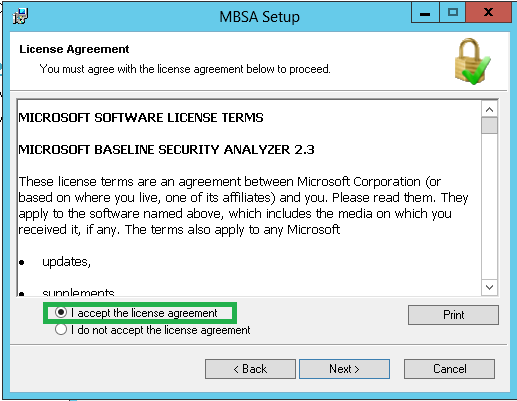
**Running the installer**

We can now run the installer corresponding to our language and architecture. The following window will pop up

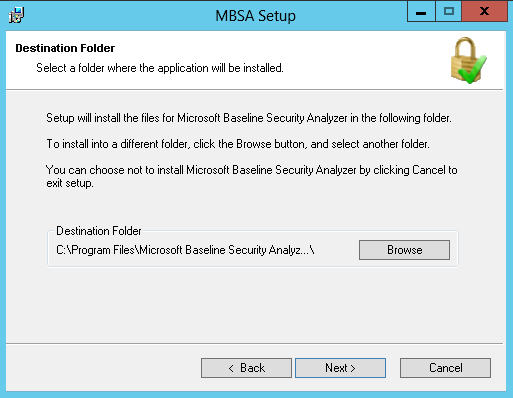


Just click on “Next” button.

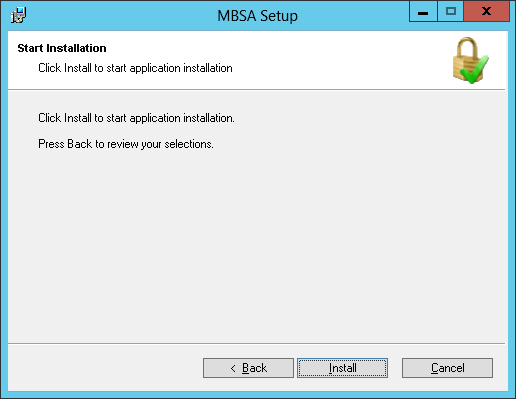
The next panel is the license agreement you will have to approve and click on “Next” button:



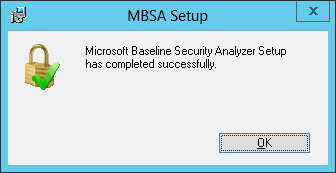
Now we must choose the destination directory. We can let it to its default or change it then click on the “Next” button:



Now we just have to confirm the install and let it run by clicking on the “Install” button:



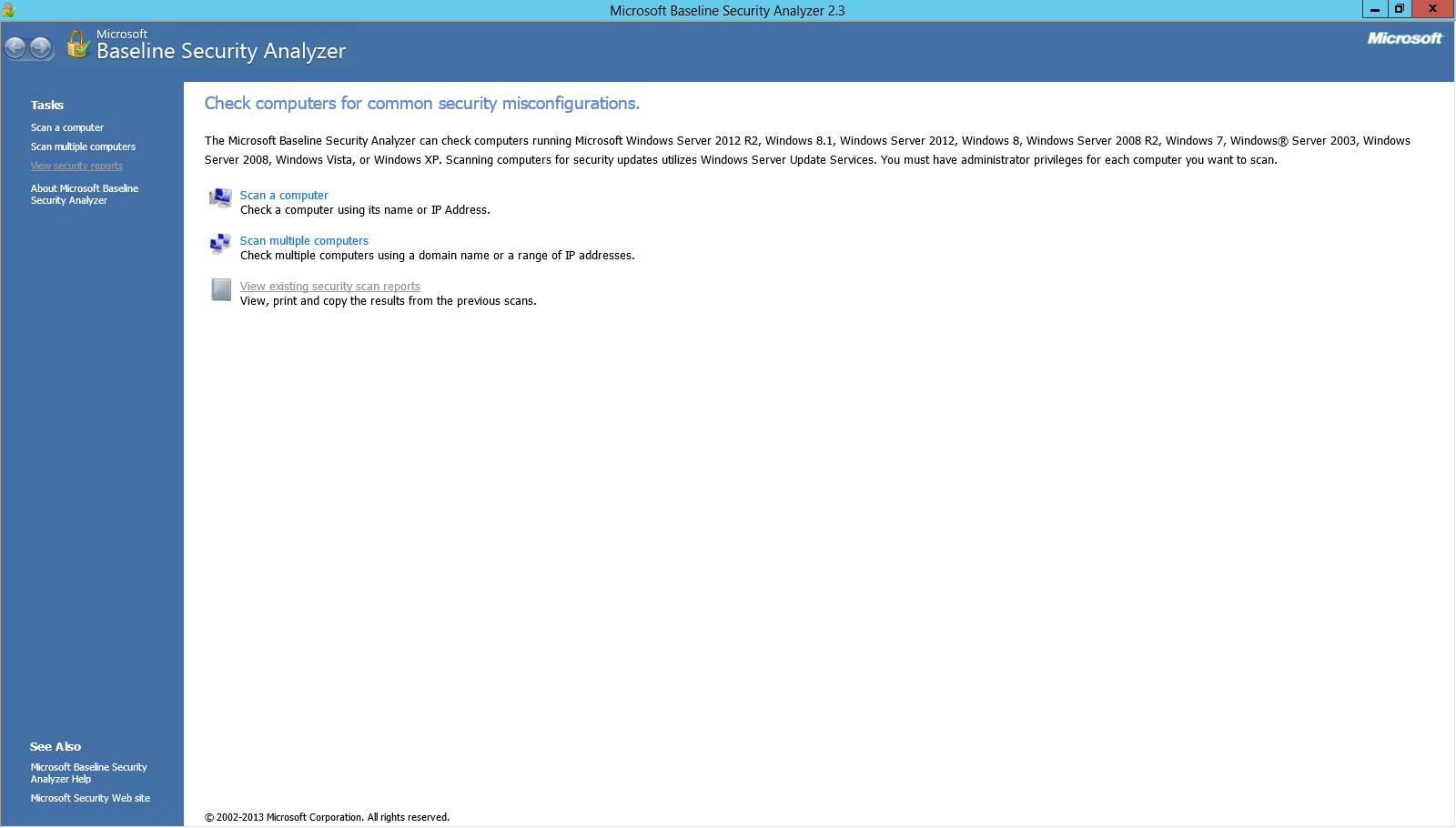
Once the installation is done, you’ll get the following popup on which you just have to click OK:



Congratulations, Microsoft Baseline Security Analyzer is now installed. Let’s now see how to use it.

## Running the tool graphically -

Let’s run it and see what the graphical interface look like:

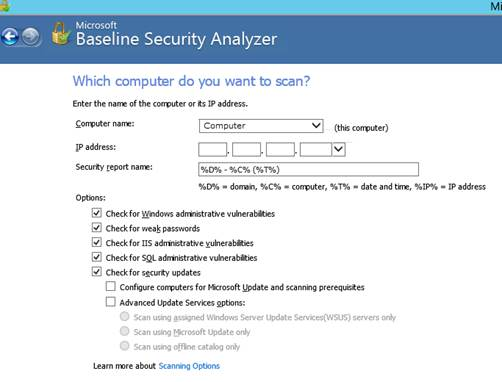


As we can see directly from the image above, this tool can:

* Scan a single computer by providing an IP or its NetBIOS name.
* Do this scan for a group of computers
* Have a look at existing reports (when we have some)

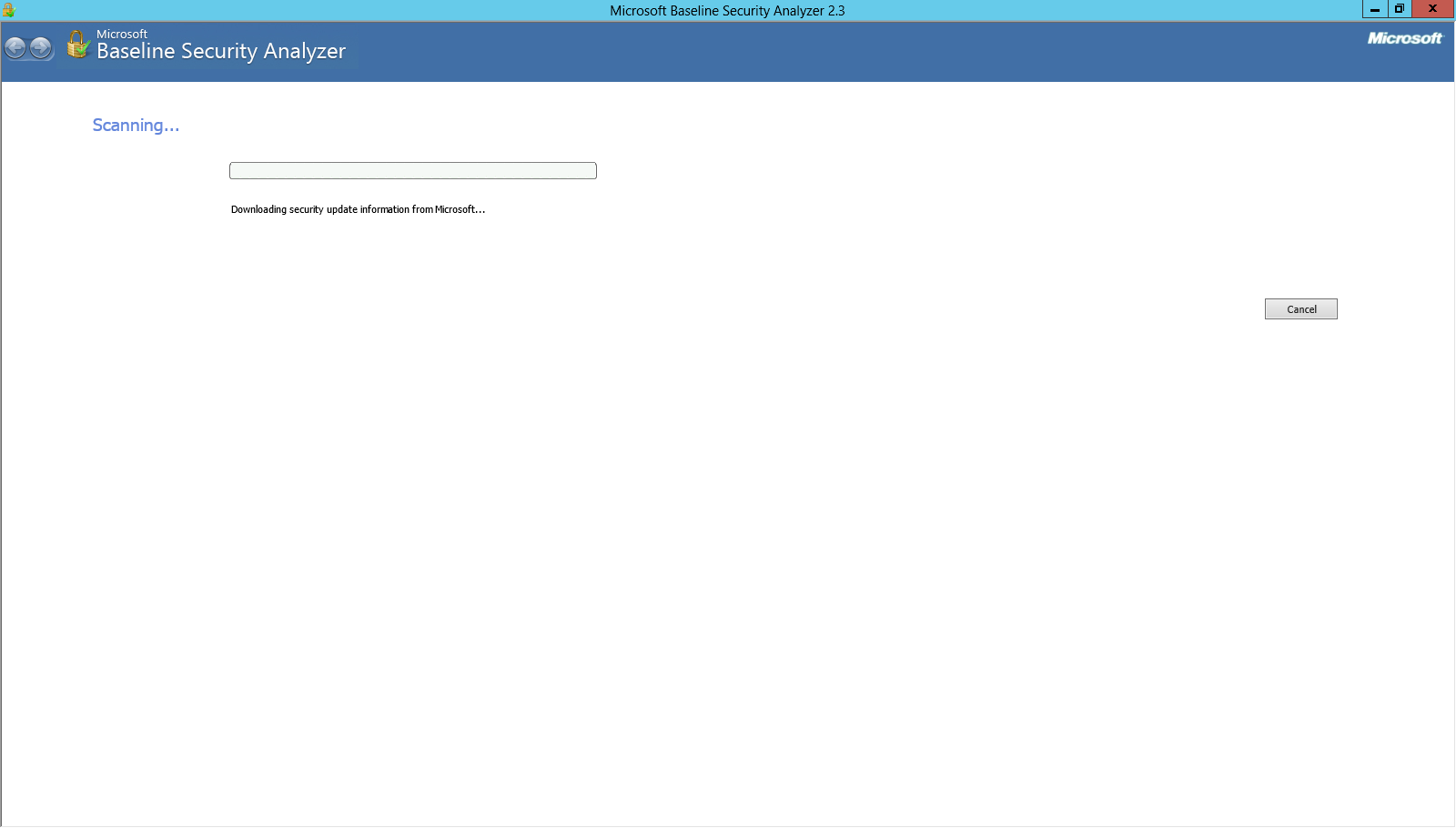
Let’s just click on “Scan a computer”:

This switches to another dialog, where you’ll need to provide some parameters. The parameters are a NetBIOS computer name, an IP address and the name of the final report which is can be parameterized. In addition, we can check or uncheck options. These options will change the behavior of MBSA. They are shown in the following image:

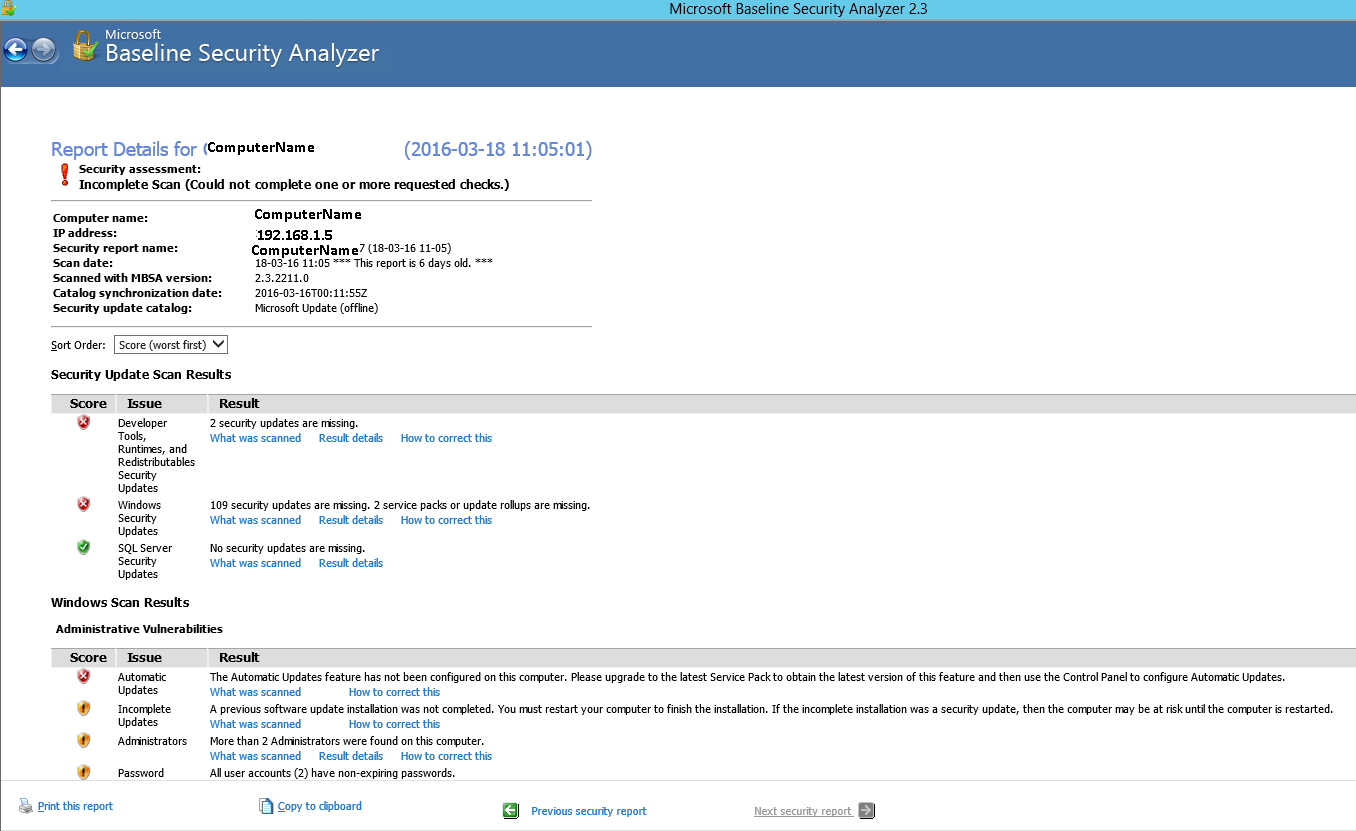


Once everything is set up appropriately, you’ll find a button at the bottom right of the screen called “Start scan”. Just click on it.

Here we go. The process can take several minutes.

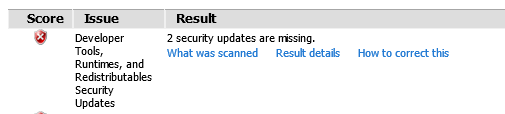


It took approximately 10 minutes to complete without taking that much memory (16 MB) or CPU (0%).



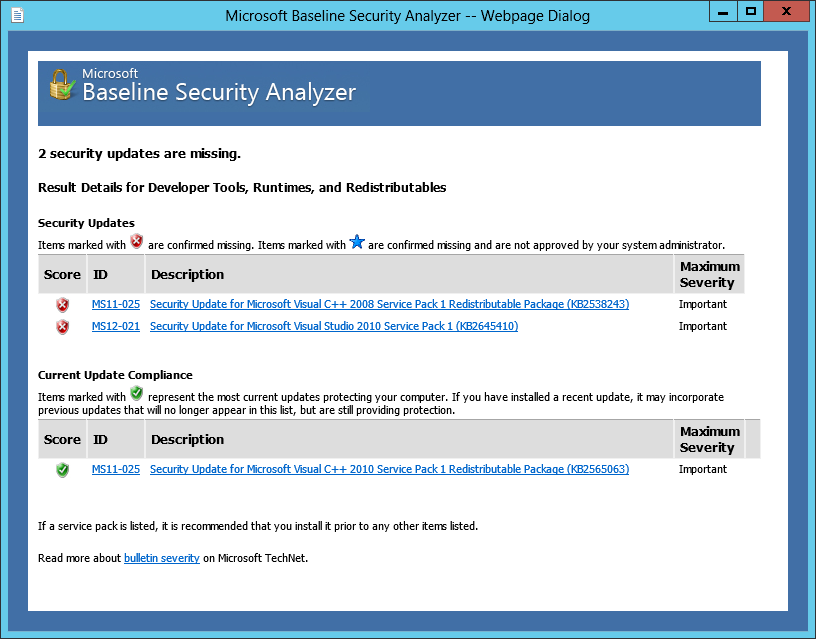
 I have to go through the whole report as it’s not an all green “everything is OK” message that is given by MBSA.

One thing we can see is that the report is organized by default with “worst first” which is to me very valuable. The next thing that is really helpful is that for every scan issue, we can see at least what was scanned, in some cases a detailed report may be accessible and/or eventually a way to correct the issue:



The “What was scanned” link opens an HTML description of the scanned aspect.

The “Result details” presents a detailed report of the analysis made by MBSA. For example, you will find this dialog displayed:



The last thing we can see in the report, are the actions that we can do on the report, as shown at the bottom of the window:

* Print the report
* Copy the report to clipboard
* Switch to another report

## Other ways to run the tool: command-line

As the description stated, there is a command-line interface for the tool. Let’s introduce “mbsacli”. To run it, we have to open an invite or a Power Shell window and go to the installation directory of MBSA (or adapt PATH environment variable so that this folder is included).

Here is a sample command I used to run against a remote server:

.\mbsacli.exe -target CHULG\si-s-serv236 /n os+sql+updates+password /qt /nd